

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-024978

(43)Date of publication of application : 29.01.1999

(51)Int.Cl.

G06F 12/00

G06F 13/00

(21)Application number : 09-189320

(71)Applicant : NEC CORP

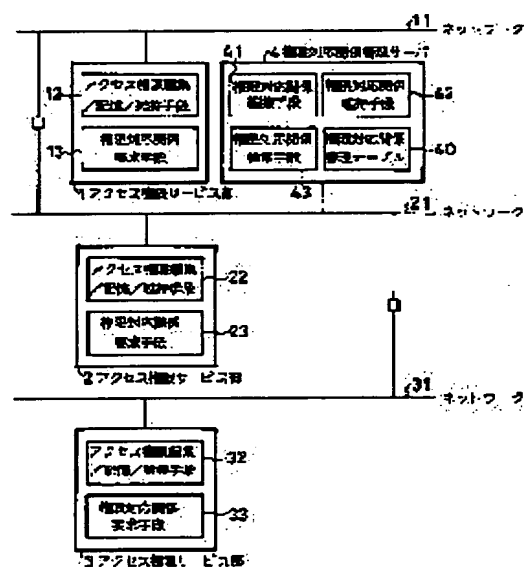
(22)Date of filing : 30.06.1997

(72)Inventor : SHOJI SHUICHI

(54) ACCESS RIGHT OVERALL MANAGEMENT METHOD/DEVICE AMONG PLURAL NETWORKS**(57)Abstract:**

PROBLEM TO BE SOLVED: To interrelate access rights of users/groups on plural different networks.

SOLUTION: In an access right correspondence relation managing server 4, an access right correspondence relation managing table 40 manages the correspondence relation of access rights on the plural networks and an access right correspondence relation compiling means 41 generates an addition record, a change record and a deletion record in an access right correspondence relation by adjusting them to the addition/change/deletion of the access right correspondence relation. An access right correspondence relation maintaining means 42 maintains/manages the access right correspondence relation managing table 40 based on the addition record, the change record and the deletion record in the access right correspondence relation. An access right correspondence relation retrieval means 43 retrieves corresponding user/group names from the access right correspondence relation managing table 40 based on the network name and user/group names of an access request source and the network name of an access request destination. When the corresponding user/group names exist, the user/group names are returned. When the corresponding user/group names do not exist, an error is returned.

**LEGAL STATUS**

[Date of request for examination] 30.06.1997

[Date of sending the examiner's decision of rejection] 11.10.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-24978

(43) 公開日 平成11年(1999) 1月29日

(51) Int.Cl.⁶

G 0 6 F 12/00
13/00

識別記号

5 3 7
3 5 5

F I

G 0 6 F 12/00
13/00

5 3 7 A
3 5 5

審査請求 有 請求項の数 7 F D (全 9 頁)

(21) 出願番号 特願平9-189320

(22) 出願日 平成9年(1997) 6月30日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 東海林 修一

東京都港区芝五丁目7番1号 日本電気株式会社内

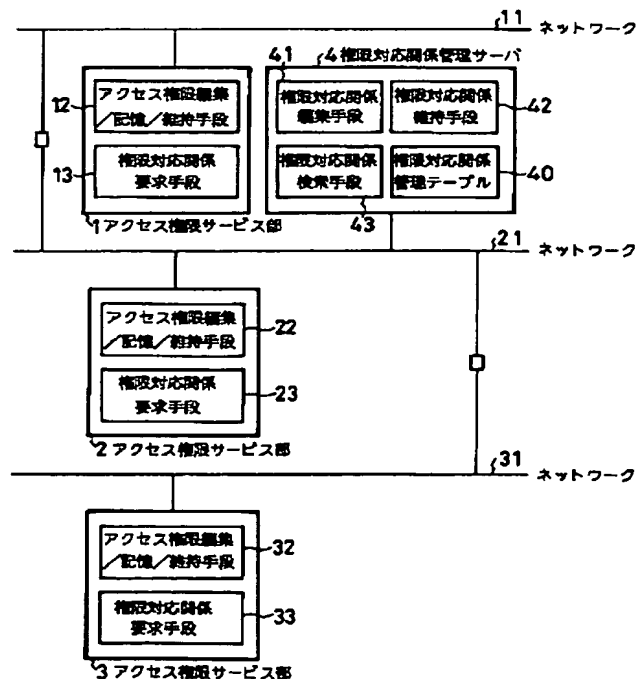
(74) 代理人 弁理士 河原 純一

(54) 【発明の名称】 複数ネットワーク間のアクセス権限統合管理方法および装置

(57) 【要約】

【課題】 複数の異なるネットワーク上のユーザ／グループのそれぞれのアクセス権限を関連付ける。

【解決手段】 権限対応関係管理サーバ4では、権限対応関係管理テーブル40が複数のネットワーク上のアクセス権限の対応関係を管理し、権限対応関係編集手段41が権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成し、権限対応関係維持手段42が権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブル40を維持管理し、権限対応関係検索手段43がアクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に権限対応関係管理テーブル40から対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す。



【特許請求の範囲】

【請求項 1】 複数のネットワークがネットワーク間接続装置を介して接続されたコンピュータネットワークシステムにおいて、

あるネットワーク上で管理されているユーザ／グループのアクセス権限を、別ネットワーク上でのユーザ／グループのアクセス権限と対応させてネットワーク上で管理することを特徴とする複数ネットワーク間のアクセス権限統合管理方法。

【請求項 2】 複数のネットワークがネットワーク間接続装置を介して接続されたコンピュータネットワークシステムにおいて、

各ネットワークに接続され自ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するとともに他のネットワーク上でのアクセス権限の対応関係を要求するアクセス権限サービス部と、

少なくとも 1 つのネットワークに接続され複数のネットワーク上のアクセス権限の対応関係を管理し前記アクセス権限サービス部からの権限対応関係要求に応じてアクセス権限の対応関係を通知する権限対応関係管理サーバとを備えることを特徴とする複数ネットワーク間のアクセス権限統合管理装置。

【請求項 3】 前記アクセス権限サービス部が、自ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するためのアクセス権限編集／記憶／維持手段と、他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段とを備える請求項 2 記載の複数ネットワーク間のアクセス権限統合管理装置。

【請求項 4】 前記権限対応関係管理サーバが、複数のネットワーク上のアクセス権限の対応関係を管理する権限対応関係管理テーブルと、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段と、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維持手段と、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段とを備える請求項 2 記載の複数ネットワーク間のアクセス権限統合管理装置。

【請求項 5】 複数のクライアントコンピュータを、各ネットワーク上におけるユーザ／グループに対応するア

クセス権限を管理するアクセス権限編集／記憶／維持手段、および他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段として機能させるためのプログラムと、サーバコンピュータを、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維持手段、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段として機能させるためのプログラムとを記録したことを特徴とする記録媒体。

【請求項 6】 コンピュータを、各ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するアクセス権限編集／記憶／維持手段、および他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段として機能させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項 7】 コンピュータを、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維持手段、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段として機能させるためのプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はネットワークシステム上のリソースへのアクセス権限の管理方法および装置に関し、特に複数ネットワーク間のアクセス権限統合管

理方法および装置に関する。

【0002】

【従来の技術】従来、この種のアクセス権限の管理方法では、コンピュータネットワークシステム上のリソースに対するアクセス権限を現実世界の組織構造に適応させるため、たとえば特開平4-302344号公報に記載されているように、情報に対するアクセス権限を示す組織データが組織の下位にあたる組織データのアクセス権限を含むことにより、現実世界の組織運営に好ましいアクセス権限の管理を可能としていた。

【0003】

【発明が解決しようとする課題】第1の問題点は、従来のアクセス権限の管理方法では、複数のネットワーク上にそれぞれが異なるアクセス権限を持つ組織構造で運用されていた場合、あるネットワーク上のリソースに対するアクセス権限を持つユーザ／グループは他の異なるネットワーク上ではリソースに対するアクセス権限を一般的には保持していないか、または元のネットワークとは異なるアクセス権限を与えられている場合があったことである。これは、異なる組織構造を基にして異なるネットワーク上でリソースへのアクセス権限の管理を行った場合に、それらの間におけるアクセス権限が関連付けられていないためである。

【0004】本発明の目的は、複数の異なるネットワーク上のユーザ／グループのそれぞれのアクセス権限を関連付ける複数ネットワーク間のアクセス権限統合管理方法を提供することにある。

【0005】また、本発明の他の目的は、複数の異なるネットワーク上のユーザ／グループのそれぞれのアクセス権限を関連付ける複数ネットワーク間のアクセス権限統合管理装置を提供することにある。

【0006】さらに、本発明の別の目的は、コンピュータを、権限対応関係管理サーバにアクセス権限の対応関係を問い合わせる権限対応関係要求手段として機能させるためのプログラムを記録した記録媒体を提供することにある。

【0007】さらにまた、本発明の別の目的は、コンピュータを、アクセス権限の対応関係の問い合わせに対して応答する権限対応関係管理サーバとして機能させるためのプログラムを記録した記録媒体を提供することにある。

【0008】

【発明を解決するための手段】本発明の複数ネットワーク間のアクセス権限統合管理方法は、複数のネットワークがネットワーク間接続装置を介して接続されたコンピュータネットワークシステムにおいて、あるネットワーク上で管理されているユーザ／グループのアクセス権限を、別ネットワーク上でのユーザ／グループのアクセス権限と対応させてネットワーク上で管理することを特徴とする。

【0009】また、本発明の複数ネットワーク間のアクセス権限統合管理装置は、複数のネットワークがネットワーク間接続装置を介して接続されたコンピュータネットワークシステムにおいて、各ネットワークに接続されるネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するとともに他のネットワーク上でのアクセス権限の対応関係を要求するアクセス権限サービス部と、少なくとも1つのネットワークに接続される複数のネットワーク上のアクセス権限の対応関係を管理し前記アクセス権限サービス部からの権限対応関係要求に応じてアクセス権限の対応関係を通知する権限対応関係管理サーバとを備えることを特徴とする。また、前記アクセス権限サービス部が、自ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するためのアクセス権限編集／記憶／維持手段と、他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段とを備える。さらに、前記権限対応関係管理サーバが、複数のネットワーク上のアクセス権限の対応関係を管理する権限対応関係管理テーブルと、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段と、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維持手段と、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段とを備える。

【0010】一方、本発明の記録媒体は、複数のクライアントコンピュータを、各ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するアクセス権限編集／記憶／維持手段、および他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段として機能させるためのプログラムと、サーバコンピュータを、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維

持手段、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段として機能させるためのプログラムとを記録したことを特徴とする。

【0011】また、本発明の記録媒体は、コンピュータを、各ネットワーク上におけるユーザ／グループに対応するアクセス権限を管理するアクセス権限編集／記憶／維持手段、および他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて前記権限対応関係管理サーバに自ネットワーク上の対応するユーザ／グループ名を問い合わせる権限対応関係要求手段として機能させるためのプログラムを記録したことを特徴とする。

【0012】さらに、本発明の記録媒体は、コンピュータを、権限対応関係の追加、変更および削除に合わせて権限対応関係の追加レコード、変更レコードおよび削除レコードを作成する権限対応関係編集手段、権限対応関係の追加レコード、変更レコードおよび削除レコードに基づいて権限対応関係管理テーブルを維持管理する権限対応関係維持手段、アクセス要求元のネットワーク名およびユーザ／グループ名とアクセス要求先のネットワーク名とを元に前記権限対応関係管理テーブルから対応するユーザ／グループ名を検索し、対応するユーザ／グループ名が存在した場合はそのユーザ／グループ名を返却し、対応するユーザ／グループ名が存在しなかった場合はエラーを返す権限対応関係検索手段として機能させるためのプログラムを記録したことを特徴とする。

【0013】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0014】図1は、本発明の第1の実施の形態に係る複数ネットワーク間のアクセス権限統合管理方法が適用されたコンピュータネットワークシステムの構成を示すブロック図である。このコンピュータネットワークシステムは、ネットワーク11、21および31がルータ、ハブ、ゲートウェイ、ブリッジ等のネットワーク間接続装置を介して接続されており、ネットワーク11にはアクセス権限サービス部1が接続され、ネットワーク21にはアクセス権限サービス部2および権限対応関係管理サーバ4が接続され、ネットワーク31にはアクセス権限サービス部3が接続されている。

【0015】ネットワーク11、21および31は、物理的または論理的に異なるネットワークである。

【0016】アクセス権限サービス部1、2および3は、ネットワーク11、21および31上におけるユー

ザ／グループに対応するアクセス権限を管理するためのアクセス権限編集／記憶／維持手段12、22および32をそれぞれ保持する。また、アクセス権限サービス部1、2および3は、他のネットワークからの自ネットワーク上のリソースへのアクセス要求があったときに他のネットワーク名およびユーザ／グループ名と自ネットワーク名とを用いて権限対応関係管理サーバ4に自ネットワーク上での対応するユーザ／グループ名を問い合わせる権限対応関係要求手段13、23および33をそれぞれ保持する。

【0017】図2を参照すると、権限対応関係要求手段13、23および33の処理は、権限対応関係問い合わせ処理（ユーザ名）ステップS001と、権限対応関係問い合わせ処理（グループ名）ステップS002と、ユーザ／グループ名返却ステップS003と、エラー処理ステップS004とからなる。

【0018】権限対応関係管理サーバ4は、あるネットワーク上で保持されるユーザ／グループのアクセス権限を、別のネットワーク上のユーザ／グループのアクセス権限に対応させる。具体的には、権限対応関係管理サーバ4は、権限対応関係管理テーブル40と、あるネットワークのアクセス権限と別のネットワークのアクセス権限との対応を作成する権限対応関係編集手段41と、アクセス権限の対応関係を権限対応関係管理テーブル40に維持管理する権限対応関係維持手段42と、アクセス権限サービス部1、2および3からの権限対応関係要求に応じて権限対応関係管理テーブル40を検索してユーザ／グループ名を返却する権限対応関係検索手段43とを有する。

【0019】図3を参照すると、権限対応関係管理テーブル40は、ネットワーク上で同じアクセス権限をもつユーザまたはグループとして、対応するそれぞれのユーザ／グループ名を保持する。また、権限対応関係管理テーブル40は、対応する名前がユーザかグループかの種別を示す情報も保持する。

【0020】権限対応関係編集手段41は、アクセス権限サービス部1、2および3により維持されるネットワーク上におけるそれぞれのユーザ／グループ名に対するアクセス権限間の対応関係を追加／変更／削除するレコードを作成する。

【0021】図4を参照すると、権限対応関係編集手段41の処理は、権限対応関係追加処理ステップS101と、権限対応関係変更処理ステップS102と、権限対応関係削除処理ステップS103とからなる。

【0022】権限対応関係維持手段42は、権限対応関係の追加／変更／削除レコードに基づいて権限対応関係管理テーブル40の権限対応関係を維持管理する。

【0023】図5を参照すると、権限対応関係維持手段42の処理は、レコード確認ステップS201と、レコード追加／変更／削除ステップS202と、エラー処理

ステップS203とからなる。

【0024】権限対応関係検索手段43は、あるネットワーク上のリソースに対して、異なるネットワーク上のユーザ／グループからのアクセス要求があった場合に、リソースの存在するネットワーク上のアクセス権限サービス部の権限対応関係要求手段からの問い合わせに対して、アクセス要求元のユーザ／グループに対応するユーザ／グループが存在するかどうかを判断し、その結果を返却する。

【0025】図6を参照すると、権限対応関係検索手段43の処理は、ユーザ／グループ名検索ステップS301と、ユーザ／グループ名返却ステップS302と、エラー処理ステップS303とからなる。

【0026】次に、このように構成された第1の実施の形態に係る複数ネットワーク間のアクセス権限統合管理方法および装置の動作について説明する。

【0027】例えば、ネットワーク11および31に、図7に示すようなユーザおよびグループの組織構造があり、アクセス権限サービス部1では、アクセス権限編集／記憶／維持手段12により、ネットワーク11上のあるリソースR（図示せず）に関してネットワーク11上のグループ1Cからの読出しを許可するというアクセス権限があらかじめ登録されているものとする。また、リソースRに関してネットワーク11上のグループ1Bおよびユーザ1Dについてはアクセス権限は登録されていないものとする。

【0028】また、各ネットワーク11、21および31の管理者は、アクセス権限サービス部1、2および3のアクセス権限編集／記憶／維持手段12、22および32に登録されるユーザ／グループ名に関して、他のネットワークに存在するユーザ／グループ名との権限対応関係を、権限対応関係管理サーバ4の権限対応関係編集手段41により権限対応関係の追加、変更および削除レコードを作成して、権限対応関係維持手段42により権限対応関係管理テーブル40に追加、変更および削除することができる。

【0029】詳しくは、権限対応関係編集手段41は、アクセス権限の対応関係の追加、変更または削除に合わせて、権限対応関係を追加するレコードを作成したり（ステップS101）、権限対応関係を変更するレコードを作成したり（ステップS102）、権限対応関係を削除するレコードを作成したりする（ステップS103）。

【0030】次に、権限対応関係維持手段42は、権限対応関係編集手段41により作成されたレコードが権限対応関係管理テーブル40にすでに存在しているレコードと内容が重複しているかをどうか（削除レコードについては削除対象となるレコードがあるかどうか）を検証し（ステップS201）、重複していない場合にはレコードを追加／変更／削除し（ステップS202）、重複

していない場合にはエラーとする（ステップS203）。

【0031】この結果、権限対応関係管理サーバ4では、権限対応関係編集手段41および権限対応関係維持手段42により、図3に示すように、権限対応関係管理テーブル40に、ネットワーク11上のグループ1Cと対応してネットワーク31上のグループ3Aが権限対応関係として登録されているものとする。また、ネットワーク11上のユーザ1Dと対応してネットワーク31上のユーザ3Eが権限対応関係として登録されているものとする。

【0032】いま、ネットワーク31上のグループ3Aに属するユーザ3Bからネットワーク11上のリソースRに対してアクセス要求が発生した場合、アクセス権限サービス部1では、アクセス権限編集／記憶／維持手段12が、自分では管理していない他のネットワーク31からのアクセス要求であるので、権限対応関係要求手段13に制御を渡す。

【0033】権限対応関係要求手段13は、アクセス要求元のネットワーク名31およびユーザ名3Bとアクセス要求先のネットワーク名11とをパラメータとして権限対応関係管理サーバ4に権限対応関係（ユーザ名）を問い合わせる権限対応関係要求を発行する（ステップS001）。

【0034】権限対応関係管理サーバ4では、権限対応関係検索手段43が、アクセス権限サービス部1からの権限対応関係要求に対して、アクセス要求元のネットワーク名31およびユーザ名3Bとアクセス要求先のネットワーク名11とを用いて権限対応関係管理テーブル40を検索し（ステップS301）、対応するユーザ名が登録されていないので、エラーをアクセス権限サービス部1に返却する（ステップS303）。

【0035】エラーを返却されたアクセス権限サービス部1では、権限対応関係要求手段13が、次にアクセス要求元のネットワーク名31およびグループ名3Aとアクセス要求先のネットワーク名11とをパラメータとして権限対応関係管理サーバ4に権限対応関係（グループ名）を問い合わせる権限対応関係要求を発行する（ステップS002）。

【0036】権限対応関係管理サーバ4では、権限対応関係検索手段43が、アクセス権限サービス部1からの権限対応関係要求に対して、アクセス要求元のネットワーク名31およびグループ名3Aとアクセス要求先のネットワーク名11を用いて権限対応関係管理テーブル40を検索して対応するグループ名1Cを取得し（ステップS301）、グループ名1Cをアクセス権限サービス部1に返却する（ステップS302）。

【0037】アクセス権限サービス部1では、権限対応関係要求手段13が、権限対応関係管理サーバ4から返却されたグループ名1Cをアクセス権限編集／記憶／維

持手段12に返却する(ステップS003)。

【0038】アクセス権限編集/記憶/維持手段12は、リソースRに関してグループ1Cには読出しを許可するアクセス権限を与えているので、ネットワーク31上のユーザ3Bからネットワーク11上のリソースRに対するアクセス要求が読出しであればそのアクセスを許可し、書込みであればそのアクセスを拒絶する。

【0039】他方、ネットワーク31上のユーザ3Eからネットワーク11上のリソースRに対してアクセス要求が発行された場合、アクセス権限サービス部1では、アクセス権限編集/記憶/維持手段12が、自分では管理していない他のネットワーク31からのアクセス要求であるので、権限対応関係要求手段13に制御を渡す。

【0040】権限対応関係要求手段13は、アクセス要求元のネットワーク名31およびユーザ名3Eと自ネットワーク名11とをパラメータとして権限対応関係管理サーバ4に権限対応関係(ユーザ名)を問い合わせる権限対応関係要求を発行する(ステップS001)。

【0041】権限対応関係管理サーバ4では、権限対応関係検索手段43が、アクセス権限サービス部1からの権限対応関係要求に対して、アクセス要求元のネットワーク名31およびユーザ名3Eとアクセス要求先のネットワーク名11とを用いて権限対応関係管理テーブル40を検索し(ステップS301)、ユーザ名3Eに対応するユーザ名1Dをアクセス権限サービス部1に返却する(ステップS302)。

【0042】アクセス権限サービス部1では、権限対応関係要求手段13が、権限対応関係管理サーバ4から返却されたユーザ名1Dをアクセス権限編集/記憶/維持手段12に返却する(ステップS003)。

【0043】アクセス権限編集/記憶/維持手段12は、リソースRに関してユーザ1Dにはアクセスを許可するアクセス権限を与えていないので、ネットワーク31上のユーザ3Eからネットワーク11上のリソースRに対するアクセス要求を拒絶する。

【0044】なお、上記第1の実施の形態の動作の説明では、ネットワーク31上のユーザからネットワーク11上のリソースにアクセス要求が発行された場合を例にとって説明したが、他のネットワーク上のユーザから別のネットワーク上のリソースにアクセス要求が発行された場合にも、同様の動作になることはいうまでもない。

【0045】次に、本発明の第2の実施の形態について図面を参照して詳細に説明する。

【0046】図8を参照すると、本発明の第2の実施の形態は、権限対応関係要求プログラムを記録した記録媒体51、52および53を備えるとともに、権限対応関係管理プログラムを記録した記録媒体54を備える。これら記録媒体51、52、53および54は、磁気ディスク、半導体メモリ、その他の記録媒体であってもよい。

【0047】権限対応関係要求プログラムは、記録媒体51、52および53からアクセス権限サービス部1、2および3にアクセス権限編集/記憶/維持手段12、22および32ならびに権限対応関係要求手段13、23および33としてそれぞれ読み込まれ、アクセス権限サービス部1、2および3の動作を制御する。

【0048】また、権限対応関係管理プログラムは、記録媒体54から権限対応関係管理サーバ4に権限対応関係編集手段41、権限対応関係維持手段42および権限対応関係検索手段43として読み込まれ、権限対応関係管理サーバ4の動作を制御する。

【0049】なお、権限対応関係要求プログラムの制御によるアクセス権限サービス部1、2、3の動作、および権限対応関係管理プログラムの制御による権限対応関係管理サーバ4の動作は、第1の実施の形態に係るアクセス権限統合管理装置の場合と全く同様であるので、それらの詳しい説明を割愛する。

【0050】

【発明の効果】本発明の第1の効果は、異なるネットワーク上に別々の組織構造でアクセス権限が管理されている場合でも簡単にアクセス権限の統合が可能となることである。その理由は、ネットワーク上の権限対応関係管理サーバで異なるネットワーク上のユーザ/グループ間のアクセス権限の対応を管理するようにしたからである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る複数ネットワーク間のアクセス権限統合管理方法が適用されたコンピュータネットワークシステムの構成を示すブロック図である。

【図2】図1中の権限対応関係要求手段の処理を示すフローチャートである。

【図3】図1中の権限対応関係管理テーブルの内容を示す図である。

【図4】図1中の権限対応関係編集手段の処理を示すフローチャートである。

【図5】図1中の権限対応関係維持手段の処理を示すフローチャートである。

【図6】図1中の権限対応関係検索手段の処理を示すフローチャートである。

【図7】第1の実施の形態に係る複数ネットワーク間のアクセス権限統合管理方法を説明するためのネットワークの組織構造の一例を示す図である。

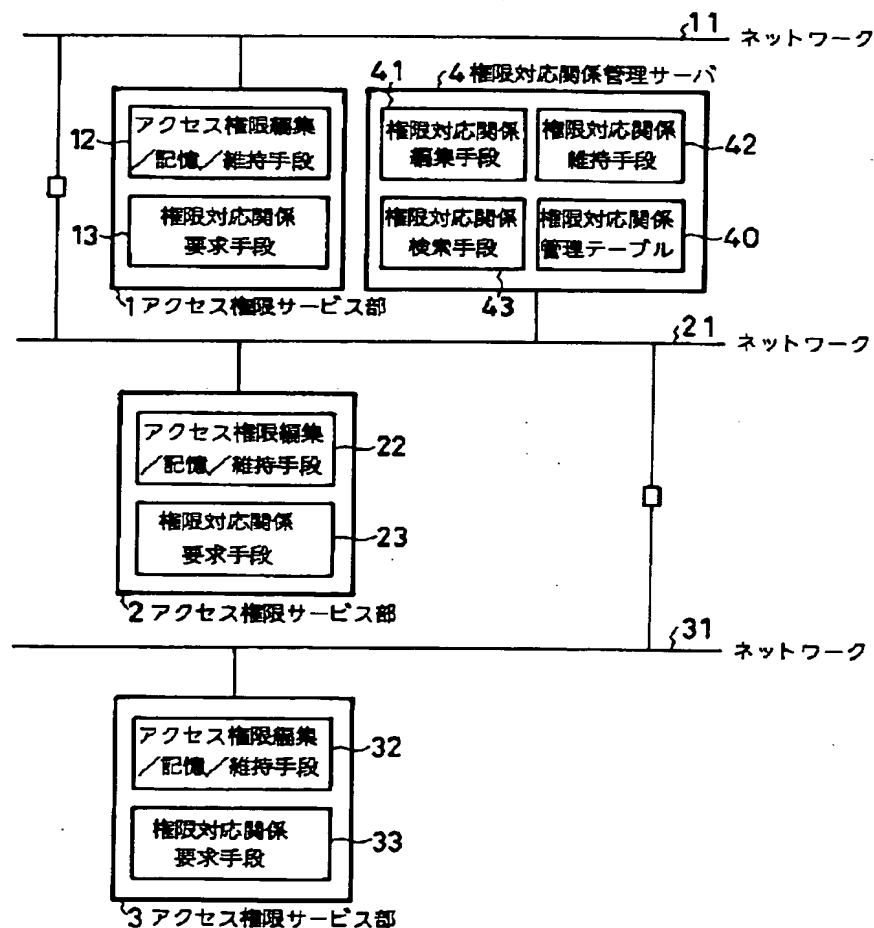
【図8】本発明の第2の実施の形態に係るアクセス権限統合管理方法が適用されたコンピュータネットワークシステムの構成を示すブロック図である。

【符号の説明】

1, 2, 3 アクセス権限サービス部
4 権限対応関係管理サーバ
11, 21, 31 ネットワーク

- 12, 22, 32 アクセス権限編集／記憶／維持手段
 13, 23, 33 権限対応関係要求手段
 40 権限対応関係管理テーブル
 41 権限対応関係編集手段
 42 権限対応関係維持手段
 43 権限対応関係検索手段
 51～54 記録媒体
 S001 権限対応関係問い合わせ処理（ユーザ名）ステップ
 S002 権限対応関係問い合わせ処理（グループ名）ステップ
 S003 ユーザ／グループ名返却ステップ
 S004 エラー処理ステップ
 S101 権限対応関係追加処理ステップ
 S102 権限対応関係変更処理ステップ
 S103 権限対応関係削除処理ステップ
 S201 レコード確認ステップ
 S202 レコード追加／変更／削除ステップ
 S203 エラー処理ステップ
 S301 ユーザ／グループ名検索ステップ
 S302 ユーザ／グループ名返却ステップ
 S303 エラー処理ステップ

【図1】

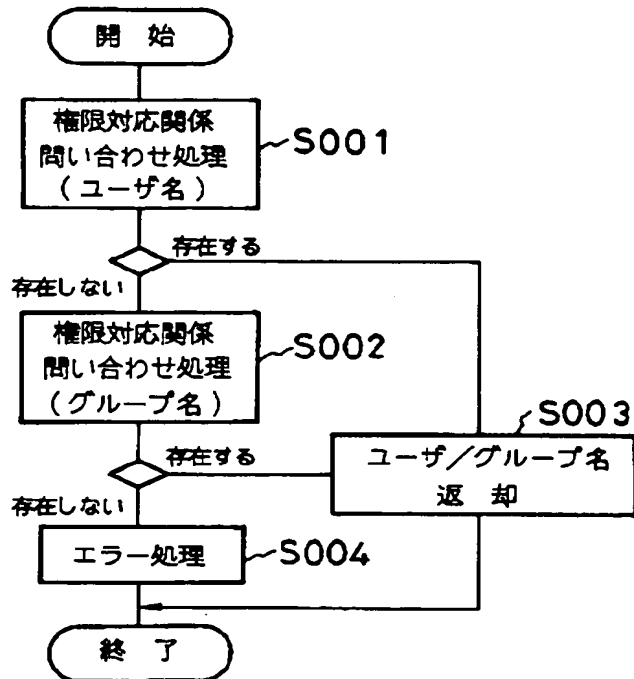


【図3】

40 権限対応関係管理テーブル

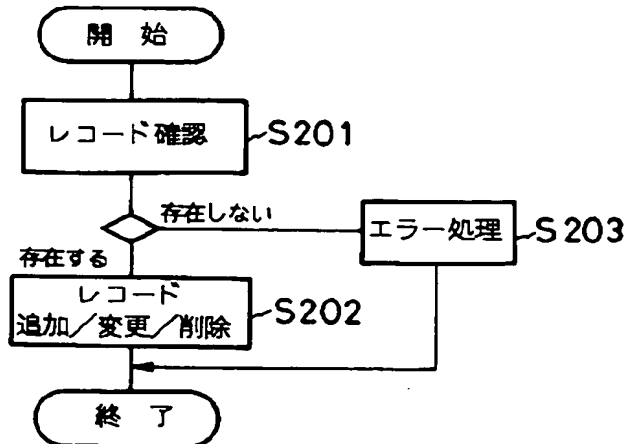
種別	ネットワーク名1	名前1	ネットワーク名2	名前2
1 グループ	ネットワーク11	グループ1C	ネットワーク31	グループ3A
2 ユーザ	ネットワーク31	ユーザ3E	ネットワーク11	ユーザ1D
	...			

【図 2】

権限対応関係要求手段
13, 23, 33

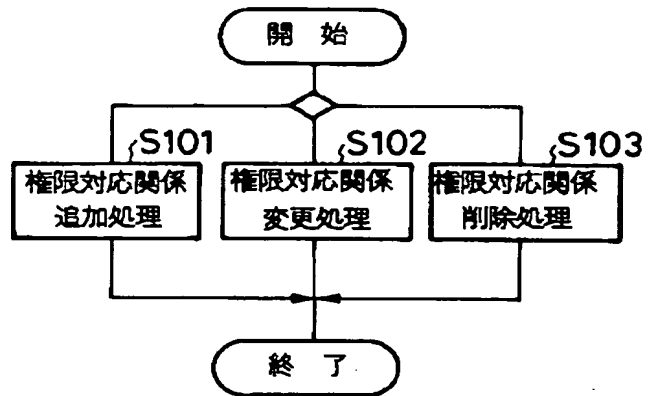
【図 5】

権限対応関係維持手段 4 2

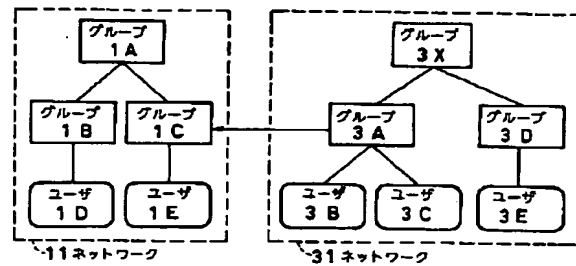


【図 4】

権限対応関係編集手段 4 1

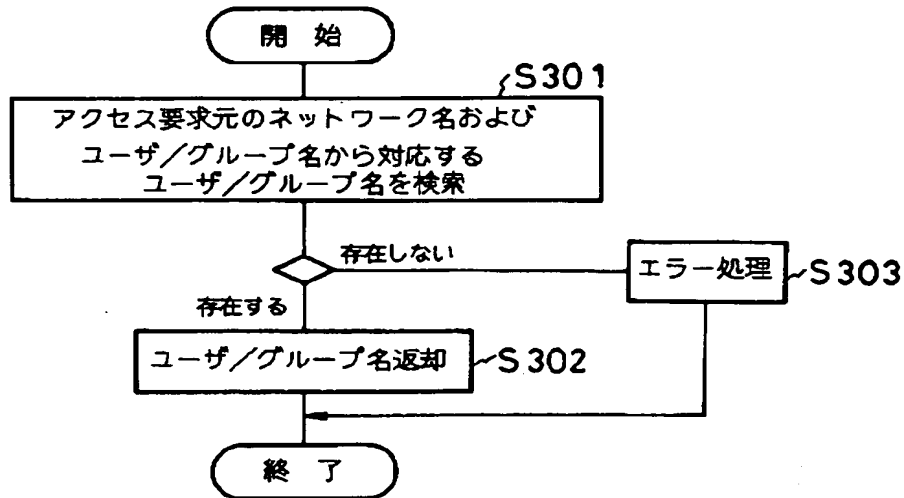


【図 7】



【図6】

権限対応関係検索手段43



【図8】

